ENCLOSURE (C)

COMPUTER SECURITY AND PRIVACY PLAN (CSPP)

OUTLINE

June 1998

HQ PLAN NO:

COMPUTER SECURITY AND PRIVACY PLAN (CSPP)

Organization:		Date:
System Type:	( ) General Support System ( ) Major Application ( ) Networked System	
Category:	( ) Mission-Essential ( ) Sensitive	
Location:	( ) DOE Germantown ( ) DOE Forrestal ( ) Other	Room No:_____

PART I SYSTEM IDENTIFICATION

A. System/Application Responsibility	
ACPPM:	TELEPHONE: ( ) -
B. System/Application Name/Title:	
C. General Description:	
Hardware Equipment/Model No:	
System Software Name(s)/Version No(s):	
Purpose:	
D. Special Security Considerations:	

PART II SENSITIVITY OF INFORMATION HANDLED

E. Sensitivity Description	
1. Confidentiality: Low ( ) Medium ( ) High ( )	Reason:
2. Integrity: Low ( ) Medium ( ) High ( )	Reason:
3. Availability: Low ( ) Medium ( ) High ( )	Reason:

PART III SYSTEM SECURITY MEASURES	
F. Risk Management:	Date Last Conducted:_____ Conducted By:_____ Next Scheduled:
G. Applicable Security Control Measures:	
1. Management:	
2. Acquisition/Development/Implementation/Installation:	
3. Operational:	
4. Technical Controls:	
5. Application Controls:	
H. Security Awareness and Training:	
I. Complimentary Controls:	

PART IV ADDITIONAL COMMENTS
J. Previous and Planned Assessments and Reviews:
1. Date Compliance Review Conducted:
Conducted By:
2. Date of Last System/Application Audit:
Conducted By:
3. Date System Previously Approved:
Approving Authority:

K. Date of Current Contingency Plan (if required): Next Revision:
Developed By:
L. Major Applications and Owners:
M. Additional Responsibilities:
1. Telecommunications Security:
2. Classified Computer Security:
3. Mutual Security Agreements:
4. Employee/Contractor/Consultant Access/Compliance:
N. Location of System/Application Documentation:
O. Remarks:

System Plan Approval:_____ Program Manager Organization	Date:

COMPUTER SECURITY AND PRIVACY PLAN (CSPP)

Organization. Enter the organization NAME on the worksheet.

Date. Enter the plan completion date.

System Type. Enter the type of host system or major application.

- General Support System
- Major Application
- Network System (may be LAN, WAN, mainframe, etc.)

Category. Indicate whether the system or application is mission-essential, sensitive, or both.

Location. Enter the physical location of the system. Include the building and room number.

PART I, SYSTEM IDENTIFICATION

Item A, System or Application Responsibility

Enter the name and telephone number of the responsible Assistant Computer Protection Program Manager (ACPPM).

Item B, System or Application Name/Title

Enter the name, and acronym (if any), of the system or application.

Item C, General Description

List the type and model of the host computer, system software operating system(s), and/or application. Provide a brief description of the purpose of the system/application (e.g., payroll, training). Include details of hardware, software and configuration/topology.

Item D, System Environment (Special Security) Considerations

Enter any special considerations that may impact the security of the system. Examples of special considerations include:

- Are there special system owner security requirements such as mandatory encryption or no contractor access.?
- Is the system accessible by the general public or shared with other users external to the organization?
- Does the system reside in a harsh environment such as dust or dampness, etc?
- Has the warranty or support agreement expired or will it expire in the near future?
- Is the system/application compliant with Year 2000 requirements?

PART II, SENSITIVITY OF INFORMATION HANDLED

Item E, Sensitivity Description

There are three areas of consideration that can contribute to the degree of security controls a sensitive or mission-essential system or application requires. Indicate whether the protection required is high (essential), medium (important), or low (minimum) in each of the listed categories and make a brief statement why.

1. **Confidentiality**. This is a statement as to level of information confidentiality as determined by the information owner. Also include any specific applicable laws or regulations that require compliance.

2. **Integrity**. Determine whether modification or incompleteness of information would limit the usefulness of the data.
3. **Availability**. Consider the importance of immediate availability of systems, such as the LAN, Payroll or scheduling.

PART III, SYSTEM SECURITY MEASURES

Item F, Risk Management

State if and when the last risk management process was conducted, who performed it and the location of the documentation. If the process has not been completed within the last three years, enter the approximate date when it will be accomplished.

Item G, Applicable Security Control Measures

Security controls apply to all computer systems, major applications and networked systems. A major application system may be running on a general support system or a network. The type and extent of security features will vary dependent on the ability of the owner/user to control the security of the system or application. Indicate whether the control is in place or planned.

1. **Management**. Indicate if security responsibility for the system or application is assigned formally in writing. Also state the policy for security screening of personnel requiring access to the system or application.

2. **Acquisition, Development, Implementation, and Installation**. State if security specifications, design review, and testing were/are part of acceptance prior to implementation. Indicate if software security certification was completed for applications. Indicate features incorporated during installation, like using cleared contractors or security supervision.
3. **Operational**. List the daily procedures and mechanisms used to protect operational systems and applications. You may refer to a standard operating procedure if it is readily available. See examples in the NIST Guide in section III.E.3

4. **Technical Controls**. The hardware and software controls that protect the computer system from unauthorized access or misuse. They help detect security violations and support security requirements for associated applications. Examples can be found in the NIST Guide in section III.E.5.

5. **Application Controls**. List the controls used to protect other system resident applications or connected systems from an active application. See Section 5 of this Plan and NIST Guide Section III.E.5.a.

Item H, Security Awareness and Training

Enter the general type and frequency of user/management security training on this system specifically. This may be terminal resident interactive security indoctrination at predetermined time intervals. Examples can be found in Section 9 of the Plan, and NIST Guide Section III.E.4.

Item I, Complimentary Controls

List any known security features provided by a supporting system that is external to the management or control of this particular system or application. Security feature examples include a mainframe with the ACF2 shell, applications containing unique file protect feature, and a server with a password feature while the individual terminal access has a system lock feature.

PART IV, Additional Comments

Item J, Previous Planned Inspections, Reviews, Audits, and Surveys

What inspections, reviews, audits, and surveys have been conducted or are scheduled on the system or application? When were they conducted? What is the designation of the official who performed them? Where are the results located?

- **Date Compliance Review Conducted.** Indicate who conducted a security compliance review and when.

- **Date of Last System/Application Audit.** When was the system or application last audited and who conducted it.

- **Date of System/Application Approved.** Enter the date and approving authority if the system or application has been previously approved for processing sensitive information.

Item K, Date of Current Contingency Plan

Enter the date and developer of the applicable contingency plan, if required. If one has not been documented, enter the approximate date when one shall be published.

Item L, Major Applications and Owners

List major applications residing on the system. Indicate if the system supports external systems or users. Attach a copy of Enclosure (A), DOE Headquarters General Support System/Major Application Security Certification and Approval, for all major application.

Item M, Additional Responsibilities

Indicate whether there are any letters, memorandums of agreement or verbal understandings with other organizations on security responsibility for the system or application.

- **Telecommunications Security.** Enter the name of the person/office responsible for telecommunications security, if applicable.

- **Classified Computer Security.** Enter the name of the CSSO, HSO, or individual who has responsibility for security of classified material. This person would be contacted in the event of inadvertent contamination of the unclassified system or application with classified information.

- **Mutual Security Agreements**. List the existing letter(s) of understanding (LOU), memorandum(s) of understanding (MOU), letter(s) of agreement (LOA), or memorandum(s) of agreement (MOA). Examples of this are as follows.

  a. System A accesses System B for specific information. System A must subscribe to the security procedures for System B.

  b. A sub-system accesses a major application system for specific fields of data. The restrictions of handling the data must be understood by the security administrator of the accessing system.

  c. A network enters a second network to access a third network. Identify who has the system security responsibility.

- **Employee/Contractor/Consultant Access and Compliance.** Provide a brief summary of requirements and procedures, such as application for, and termination of, access privileges applicable to employee, contractor or consultant access to the system or application.

Item N, Location of System/Application Documentation

Identify the location of the system or application documentation and who maintains it.

Item O, Remarks

Use this portion for any additional comments or remarks not covered in this checklist that would have an affect on the security posture of the system or application. It may also be used to expand upon other input to the worksheet.

System Plan Approval

The system plan must be approved by the Federal Program Manager responsible for the functional area the system is supporting.